(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 March 2005 (17.03.2005)

PCT

(10) International Publication Number
WO 2005/024567 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2004/026809

(22) International Filing Date: 18 August 2004 (18.08.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/496,088	18 August 2003 (18.08.2003)	US
60/539,242	26 January 2004 (26.01.2004)	US
60/581,507	21 June 2004 (21.06.2004)	US

(71) Applicants and
(72) Inventors: **SPEARMAN, Anthony, C.** [US/US]; Route 2, Box 39, Lane, SC 29564 (US). **WASHBURN, E., Russell, III** [US/US]; 3709 Church Street Ext., Roebuct, SC 29376 (US).

(74) Agent: **ALEXANDER, Tony, D.**; Post Office Box 1728, Evans, GA 30809 (US).

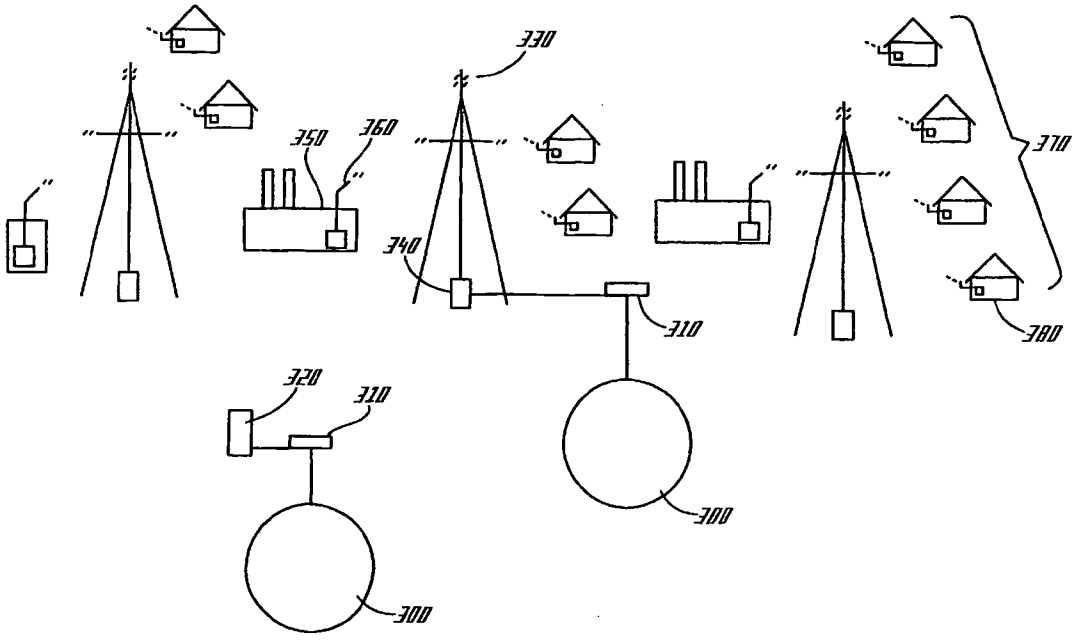
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*
— *of inventorship (Rule 4.17(iv)) for US only*

[Continued on next page]

(54) Title: NETWORK COMMUNICATION SECURITY SYSTEM, MONITORING SYSTEM AND METHODS



(57) Abstract: A system and method of intrusion detection and stoppage that prevents ARP spoofing while preserving the dynamic nature of the network. In particular, a method of turning off ARP without having to resort to static routes and static ARP entry on each computer is provided. Moreover, the system and methods provide for content filtering of both text and images and remote device monitoring and actuation.

WO 2005/024567 A2

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

NETWORK COMMUNICATION SECURITY SYSTEM, MONITORING SYSTEM AND METHODS

FIELD OF THE INVENTION

The present invention relates generally to network security and more particularly to a system and a method of providing ARP tactic resistant security for wireless and wired networks in addition to filtration and remote monitoring systems and methods.

BACKGROUND OF THE INVENTION

With the advent of the free use policy of the microwave frequency of 2.4Ghz, several companies set out to develop a means to connect computers to central hubs within single or multiple facilities. As a result, wireless local area networks became very popular within select segments of the economy.

However, wireless equipment was designed to service private LANs and the need to extrapolate to wide area networks has led to the manifestation of several limitations. In particular, the 2.4 Ghz frequency solution has lagged behind wired connections in terms of speed and volume of transmissions since its inception. It has also been discovered that water has a significant impact on transmissions of the 2.4 Ghz spectrum. With this in mind, it is no surprise that the foliage of trees can attenuate signal strength to unacceptable levels. Additional concerns have been raised regarding routing efficiency, public domain access control, bandwidth control, data interception, and basic security.

In reaction to these limitations, companies have recently developed wireless equipment that is capable of speeds up to 11Mps but have been unable to address the control issues listed above. Of particular importance is security.

One form of security provided that the security information be held confidential and released to authorized users only, in the form of the network name. However, the wide dissemination of the network name makes security in public domains virtually impossible. The next generation security method employed MAC filtering. MAC filtering also proves of little consequence in a public domain because of the basic premise of an open wireless system. Traffic on a wireless system is not logically separated between nodes. Therefore, message traffic may be sniffed and decoded. MAC address spoofing is a common hacker method of creating aliases. Furthermore, the MAC address filtering occurs on the connection point to the wireless equipment. This poses two threats.

First the user can connect to the node. Once connected to the node, network traffic may be passed to other users on the node. Moreover, if any user has established a proxy server on an authorized connection, the invalid MAC address may pass through the open proxy. This step can be done with or without knowledge of the user with the proxy.

Second, although theft of service is simple with MAC addressing, another fundamental security issue arises regarding access control. In conventional wireless equipment, the MAC address filtering occurs at the connection point. The connection point typically contains approximately 400 to 500 available MAC address filters. This theory of limited MAC addresses is good for stationary

customers but is very limiting on roaming customers. Without placing every customer on every connection point, mobile use is impossible.

A central MAC server could alleviate this problem, but would create the environment for an alternative security breach resulting from the clear text passage of authorized MAC addresses.

In an attempt to address the limitations of MAC addressing, vendors have provided RADIUS like solutions for MAC addressing. However, RADIUS creates a severe problem for mobility at the socket layer for the network. The user will experience short interruptions in service as they transition towers. This is fine for some forms of Internet traffic, like FTP, but Simple Mail Transfer Protocol (SMTP) and streaming video/audio are adversely effected and will lead to service interruptions.

Additionally, Wired Equivalent Protocol (WEP) is used as a security feature for precluding the interception of traffic. This protocol is of little use in a public domain. WEP is a common key code solution that allows the user to store the encryption key in clear text in the user computer. It is a very simple process to extract this key code from one computer to another in a public domain. In a private setting this code control is an operational security measure that will result in an efficient means of security. However, this operational security is not feasible in the public sector. WEP also places 40 percent of overhead into the network greatly reducing the effective bandwidth available to customers.

Finally with all these items addressed there still resides the problem with routing the entire network. Today's routing logic only addresses 3 to 5 bridge layers in any given data network. In order to properly build out a location requires many more than 3 to 5

connection points within a city. To solve the WPDWAN requires a wireless router on critical nodes.

But, even with the routing layer solved the inevitable out point arises with mobile customers. In today's network design each computer connected to the network requires an IP address. That address is assigned when the first communication of authentication is completed. We can assume that the network will not be on a contiguous network with all connection points leading to one out point. This design is neither logistically feasible on a large scale nor is it a functionally redundant design. Networks are designed to physically segment networks for redundancy. When that is completed the network has border routing involved that transports information from the LAN to the Internet. The border router has a logical segment of addresses that it routinely routes. However, mobile IP is not typically included in this method because to date most LANs have been static in nature. The IP address can be assigned through DHCP or assigned as static. In either case that IP is assigned to the logical and physical segment in which it was assigned. In order to route in another segment area the IP address must be reassigned. If this scenario is used then static IP addressing no longer becomes an option. However, if the border routers broadcast all border routes, it is possible to carry IP addresses from one physical border segment into another border segment. In that scenario both DHCP and static IP addressing are functional solutions. This method can be accomplished using Border Gateway Protocol (BGP). However, this solution requires that the wireless connection and route be one layer removed from the border router. Hence a WPDWAN with mobile solution cannot be accomplished without BGP, and a multi-point wireless router.

Physical segments will naturally be created in the build out of a cellular network that will coincide with a logic separation of routing paths. It is conceivable that each customer would receive his or her own static IP. This method is used in Europe. However, that process is cumbersome, logistically difficult to handle, and a waste of resources. DHCP is the alternative to distribute IP addresses to those users that are online and using the service. Under the auspice of DHCP submission it now becomes difficult to manage IP addresses as users pass from one physical segment to another. However, there is a dynamic network solution not innate to any operating system but developed by a third party that can dynamically shift these addresses to work between the physical and logical segmentation. Furthermore this same system offers directory services ability giving the network engineer the ability to control access at different locations with different bandwidth and rates of service.

To date, high bandwidth wireless providers have attempted to provide everything from licensed frequencies to optical transports. Many of these products have not taken hold in a wired world. The expenses associated with licensed frequencies make it difficult to build out large infrastructures. The optical solutions must have direct line of site and have proved difficult to route the network.

Wired networks today address all of these issues. Network management is passed through secure channels logically separated from user traffic to prevent administrative sniffing. Furthermore authentication is completed using RADIUS demanding a usemame and password, which is done at a central server as opposed to endpoint connections. Therefore updates to directory structures and routing solutions are solved when the user authenticates. In a wired

network there is no need for mobile IP and the requirements for BGP are limited to redundancy issues.

Therefore, there is an existing need for a next generation of wired-like network solution to address the wireless communication challenges of today's public domain wide area networks.

In order to manage a wireless connection point, SNMP protocol became the standard method for data transfer. To modify the MAC filter, the administrative password for the access connection point is passed along the network. This password is passed in clear text. Without secure shell connections this clear text message becomes easy to intercept for anyone connected to the WAN. Once the administrative password is breached the whole system becomes compromised. Earlier systems prevented this by providing only those within the organization the network name. Without the network name, wireless cards will not connect with the connection point. In a public domain environment the network name will be common to all those that use the service, which makes unauthorized access relatively simple. Additionally, users of the public domain environment would like to have the freedom of having quicker data transfer as a result of having undesirable content filtered. Moreover, the user would prefer not to have to install filtration software on their mobile computing device because of the memory and processing speed impact as well as the ineffectiveness of most filtering software. This is particularly evident with image filtering.

Current image filtering techniques fall into three categories, namely, contextual text filtering, URL filtering and image color scheme filtering. Contextual text filtering principally attempts to filter pornography and objectionable content by screening the text

associated with an image file without analyzing the image itself. Unfortunately, the lexicon of pornography overlaps significantly with that of more benign discourse, which can either lead to frequent false-positives or ineffective screening.

URL filtering is the practice of compiling an exhaustive list of websites at which objectionable content can be viewed or from which objectionable content originates. The difficulty with this method is the inability to keep up with new and changing locations of objectionable material.

Image color scheme filtering attempts to evaluate skin tones and body shapes in images to screen pornography from more innocuous images. Unfortunately, such methods can rarely distinguish between a baby photo and what is traditionally defined as pornography; particularly, in the case of child pornography. Additionally, there are objectionable images in addition to nudity that a user may desire to have filtered.

Address Resolution Protocol (ARP) is a TCP/IP protocol used to convert an IP address into a physical address (called a DLC address), such as an Ethernet address. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address. There is also Reverse ARP (RARP), which can be used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address. It was believed that the use of cryptographic values would allow the secure use of ARP in wide area networks. In addition, computers running the secure form of ARP should be allowed to pass ARP traffic to the untrusted host, but not be allowed to receive RARP or ARP input from those untrusted hosts.

A cryptographic checksum is a mathematical value that is assigned to a file and used to "test" the file at a later date to verify that the data contained in the file has not been maliciously changed. A cryptographic checksum is created by performing a complicated series of mathematical operations (known as a cryptographic algorithm) that translates the data in the file into a fixed string of digits called a hash value, which is then used as a checksum. It was widely believed that these cryptographic algorithms would thwart hacking under the presumption that without knowing which cryptographic algorithm was used to create the hash value, it would be highly unlikely that an unauthorized person would be able to change data without inadvertently changing the corresponding checksum. Cryptographic checksums are used in data transmission and data storage. Unfortunately, it has been discovered that cryptographic checksums (e.g., message authentication codes, integrity check-values, modification detection codes, or message integrity codes) are also vulnerable to ARP spoofing.

Because of the utility of ARP, it is widely used in both local area networks and wide area networks. In fact, different operating systems handle ARP traffic in different ways. The most ubiquitous OS, Windows, employs ARP traffic as a kernel level driver and cannot be controlled by the user. Therefore removing ARP at the router edge point does not effectively remove ARP from the network itself. It is this ubiquity of ARP that makes it a principal tool in system intrusion. It is safe to say that in high level hacking procedures, ARP is the fundamental system flaw that is exploited to gain unauthorized access to the system. For example, "Man in the Middle" and Session Hijacking methods utilize ARP. Within Man –in-the- Middle (MIM) attacks users can obtain passwords on even secure shell (SSH) encrypted traffic. Therefore,

because of the ubiquity of ARP, DSL, Cable Modem, Hubbed, switched and wireless networks are also susceptible to these hacking methods.

Heretofore, the principal solution provided in the networking community is to turn ARP off on the network. Unfortunately, turning off ARP at the network level requires a static route and a static ARP entry on every computer. For many network users, these requisite steps make setting up the wireless network less appealing. Moreover, it deprives the network of its most salient feature, namely, dynamism. Additionally, in instances when users are hubbed together as a single node, turning ARP off on the network still does not alleviate session hijacking.

Security issues are also increasing with the proliferation of Wireless Fidelity (WiFi), otherwise known as Wireless Networking, which commonly uses the 802.11b protocol. The principal advantages of WiFi are numerous but there are shortcomings. Principally, the overall cost of updating data communications networks will decrease because of lower capital equipment expenditures. WiFi greatly simplifies the planning and maintenance process since capability can easily be added or moved by moving or adding a node. WiFi allows employees to remotely access the corporate network without reliance on a dedicated dial-up number or a VPN, but instead use the Internet to access their corporate applications with ubiquitous public hotspots.

WiFi will also have an impact on VoIP. While voice over the LAN has been possible for some time, its benefits were generally considered marginal when compared to cost of implementation including special equipment requirements and additional LAN capacity. VoIP has already shown great promise and is gradually replacing the traditional PBXs as that gear is fully amortized. The case

for VoIP, however, becomes even stronger with WiFi. The marriage of data and voice in a WLAN environment, with the full-feature capabilities of the IP PBX, is certain to be the wave of the future.

Conversely, WiFi has limitations related to its signal strength and data packet processing methods. Because of the queue and sequence process associated with WiFi, it is possible for a legitimate device to flood the system with data requests. Moreover, research indicates that, in about an hour, any skilled user with basic WiFi equipment could determine the encryption key for a corporate WiFi network by intercepting and analyzing scrambled data passing over the network from a nearby parking lot.

Unlike lower frequencies that have a diminished data rate, WiFi has a greater data rate. Unfortunately, the tradeoff is less penetration efficiency and loss of control over the access points for a particular network. This loss of network access control has frightened many network administrators, especially considering the poor security reputation of WiFi.

Controlled frequencies such as TDMA and CDMA allow users to amplify the source signal significantly higher than the WiFi spectrum as well as limit unwanted congestion in the spectrum, which enables even greater ranges despite limited signal strength on client devices.

There is a need for a piece of wireless equipment that can be used to effectively connect a large WAN or to assist with the monitoring of remote devices. There is also an existing need for a wireless provisioning device that provides network routing at the source and security measures through the network. There is an additional need for unlicensed spectrum wireless connection points that provide bridging solutions that afford the user the ability to place wireless equipment in a wide area network. There is yet another

existing need for wireless connections designed for outdoor use and flexible security. Additionally, there remains a need for a system that can accommodate multiple connections back to the wireless access point without requiring rebooting before the new roaming members can be added to the system. Moreover, there remains a need for a robust content filtration system that is capable of filtering undesirable text transmissions as well as repugnant images. It is preferable that this filtering system be capable of decoding encrypted messages disguised as images.

There is also an existing need for a system and method of intrusion detection and stoppage that prevents ARP spoofing while preserving the dynamic nature of the network. In particular, there remains a need for a method of turning off ARP without having to resort to static routes and static ARP entry on each computer.

A need exists for a system and method of providing the advantages of WiFi in networks generally and VOIP systems in particular while eleviating the shortcomings of WiFi. In particular, there is a need for a WiFi network that provides a robust authentication and access control.

Moreover, there is a need for a secure system that can be populated with the remote device identifiers such as the International Mobile Equipment Identifier (IMEI) or the International Mobile Subscriber Identifier (IMSI) that can be used for security and as a unique identifier for purposes of remotely monitoring and controling devices such as PDAs, implantable medical devices, vehicles, etc.

SUMMARY OF EXEMPLARY EMBODIMENTS

In an exemplary embodiment in accordance with the present invention, a system and method is provided that ensures users of

public domain wide area networks in particular and networks generally, secure, authenticated and dynamic access to the network.

In an exemplary embodiment in accordance with the present invention, a system and method is provided that ensures users of public domain wide area networks, preferably in the 802.11 spectrum, have secure, authenticated, mobile access to the network. In the furtherance of this and other objectives, a system is provided that does not require authorization at each tower, which demands more network overhead. Rather, instead of affecting the radio connection, the system preferably affects the network connection at the out point so as to reduce overall network traffic and maintain a single socket connection. The system may have distributed concentrated points of authentication, that does not interfere with the transient capabilities of the 802.11 spectrum, to reduce server loads and enhance demographic scalability.

It is a principle objective in accordance with the present invention to provide a method and system of network security for public domain wide area networks so as to provide a virtual private network between client and route controllers, preventing data interception by outside sources. In the furtherance of this and other objectives, a wireless provisioning device is provided that allows the use of individual key code via IP Security VPN. Unlike WEP, which used common key code, the present system and method reduces overhead by about 40%. Also, by using the wireless provisioning device, the present system and method allow remote control of access and bandwidth by the LDAP server. Moreover, the LDAP replication standard enables the definition of profiles for users to control bandwidth and security in a demographically scalable fashion.

An additional objective of an exemplary embodiment of the present invention is to provide a system and method that precludes, at best, and limits the duration of, at least, unauthorized use. In the furtherance of this and other objectives, the system and method employs dynamic route allocation, which provides that there is no standard route for an IP address, rather the route is determined at the time of addressing. Moreover, if conflicts arise in the system, a valid address will be reissued and client access will resume.

Yet another objective of the present invention is to provide a system and method that can utilize multiple vendor equipment. Since authentication by radius requires a client side driver, card and drive compatibility issues arise. However, a system and method in accordance with the present invention does not require a client side driver and therefore can be used promiscuously with diverse vendor equipment.

The "Man In The Middle" attack is a well-known attack methodology where an attacker sniffs packets from the network, modifies them and inserts them back into the network. ARP spoofing involves forging a packet source hardware address (MAC address) to the address of the host you pretend to be. Session Hijacking involves an attacker using captured, brute forced, or reverse-engineered authentication tokens to seize control of a legitimate user's web application session while that user is logged into the application. This usually results in the legitimate user losing access or functionality to the current web session, while the attacker is able to perform all normal application functions with the same privileges of the legitimate user. This class of attacks usually relies on a combination of other simpler Session Management attacks.

Both "Man In The Middle" and Session Hijacking attacks utilize ARP. In order to prevent these and other attacks, specifically ARP poisoning and ARP spoofing and render ARP secure, the present inventor conceived a method that in a preferred embodiment comprises a proprietary client that disables ARP when the IP Stack comes up in the operating system. In the furtherance of this and other objectives, all ARP packets would subsequently be rejected. Moreover, this client side application makes UDP packet request looking for a public and private key from the server to establish static ARP on route controller and the user's PC, while allowing client DHCP requests without ARP entries on the route controller. As a result, all data must travel from user's PC to the route controller through an IPSEC tunnel created before authentication takes place, which makes auditing and IDS more robust due to the fact that all data packets are evaluated by an intelligent router.

A bad packet list is created and the route controller only lets packets through that are not on the list. The IDS system detects source, destination and modus operandi (i.e., signature) of the hack. Individually benign data may be allowed through but as a coordinated group of data's score increases to a predefined score parameter during a predefined period of time, subsequent access is blocked. This differs from conventional systems in that the audit function is not localized allowing the every data packet to be screened at the same location.

A principal objective of a preferred embodiment of the present invention is to provide an easy to use authenticated system. On the initial login, public and private keys are passed between the client computer and the provisioning device (as described in U.S. Patent Application Serial No. 09/660,709, which is incorporated in its entirety

by this reference) and deployed in a system, for example like the one disclosed in co-pending U.S. Patent Application Serial No. 10/223,255 (which is incorporated in its entirety by this reference). Both sides use these keys to generate trusted certificates, which are passed between the two devices. In the furtherance of this and other objectives, the username and password do not have to be retyped into the SSL layer every time a session is initiated, rather they can be saved into the client. Additionally, an IP table entry is made on an intelligent router to make the route effective and allow entry.

An additional objective in accordance with the present invention is to provide an enhanced audit function. A preferred audit system tracks all data packets and puts them into a relational database, which stores only unique entries. Furthermore, the controlling nature of the ARP structure is managed by a policy table. With such implementation individual machines can be restricted to a table of other machines and ports for activity. With this feature port level control similar to a self-managing firewall can take place between two or more computers that are hubbed together. Coupled with a heuristic set that evaluates DNS resolution of all of the material accessed. DNS Fails messages are generally an indication of unwanted data on the system (e.g., outbound zombies). This method can be used to control SPAM and spyware. Unlike spam filters that focus on the spam data itself, the present method filters spam and spyware by limiting IP addresses allowed on the system, essentially the system blocks the servers that send the spam.

There is an additional objective in accordance with the present invention, which provides a method of optimizing bandwidth by limiting spam source server and unwanted transmittal from zombies, bots and spyware access to the system. Statistically, a quarter of any

network's data traffic is unwanted data. By blocking the server that originates the spam rather than the individual data packets, the system traffic is significantly reduced. This principally follows from the fact that packet-by-packet analysis and its concomitant bandwidth overhead allocation is not required once a server has been identified as a source of undesirable data. In many systems ARP traffic itself can be a large source of overhead. The implementation of SARP removes this form of overhead.

Yet another objective in accordance with the present invention is to provide a routing system that allows a SQL database to report upward to an intelligent router, which can propagate downward to the other routers to shut down the entire system or segmentally. Threat level scores can also give indications of perceived weaknesses in the system so they can be rectified and render the system less desirable of a target.

Still another objective of the present invention is to provide wireless connections designed for outdoor use and flexible security. The present invention achieves the above objective through each of several embodiments, particularly, by radius authentication. Radius authentication is a more universal, more flexible and more secure method of authentication. The authentication process is done with secure connections to a central server. If for some reason security is breached then the username and password can be changed on the server side through a database change as opposed to a hardware change. By incorporating a new operating system with the use of the present wireless cards, wireless devices can be configured for logical management through secure connections. Furthermore, radius authentication can pass securely through the wireless device into the secure network.

An additional objective of the present invention is to provide a system that can accommodate multiple connections back to the wireless access point without requiring rebooting before the new roaming members can be added to the system.

In accomplishing these and other objectives, there has been provided, in accordance with one aspect of the present invention, a wireless provisioning device that can route at the node providing for lower network overhead and stabilizing the network into a durable redundant WAN.

Yet another objective in accordance with certain embodiments of the present invention is to provide a filtering system, a filtering algorithm and a filtering method to determine if content is encrypted in images and block the transmission of such messages.

Additionally, it is an objective in accordance with a preferred embodiment of the present invention to provide a system and method for monitoring devices remotely and manipulating their functionality remotely.

Further objects, features and advantages of the invention will be apparent from the following detailed description taken in conjunction with the accompanying drawings.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The Provisioning router system, in accordance with the present invention comprise a plurality of wireless access points; a wireless provisioning device for receiving, transmitting, and directing data over a plurality of networks and capable of sustaining connectivity between the wireless access points and the wireless provisioning device, the wireless provisioning device comprising a chassis, at lease one network card, at least one wireless card, at least one

processor, and at least one operating system operable configured in the chassis and associated with at least one of the plurality of wireless access points for transmitting and receiving data between the wireless access point and a carrier structure and where the wireless provisioning device is capable of accommodating multiple connections back to the wireless access point without requiring rebooting before a new roaming member can be added to the system; a carrier structure communicably positioned between the wireless provisioning device and the plurality of wireless access points for transmitting and receiving data between the wireless provisioning device and the plurality of wireless access points by means of a secure connection; and a security authentication protocol capable of authenticating traffic as it passes through the carrier structure.

The following terms are used in this application:

Access Point: On a network, a device designed to allow computers that are not part of a network to connect to and communicate with the network. The primary function of an access point is to provide a point of access for those unconnected computers.

Authentication: A system of measures for keeping information on a system safe from corruption or prying eyes. In networks, the procedure by which a computer verifies user identification. The most common form involves the comparison of a logon name and password to a stored file of approved user names and passwords. Any differences between the two will prohibit the user from accessing the information.

Bridge: Links networks so that data from one network can pass through another network on its way to still another network.

Datagram: A single unit of data, including its destination information, which is transmitted through a network.

Directory Service Member: A network management system, located on one enterprise capable computer. This computer maintains a database directory that stores all information from billing to authentication privileges for those on the network. Specifically this machine records MAC addresses and billing profiles for those in the system. This computer is a central repository that controls users access, system privileges and payment status.

Dynamic Host Configuration Protocol (DHCP): An Internet protocol for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver TCP/IP stock configuration parameters, and provide other information such as the addresses for auxiliary servers.

Gateway: A complex internetworking device that converts information from one protocol to another. Gateways transfer information between networks that use different communications protocols. The gateway actually tears down the information from one service and restructures it in the other network's protocol format. Gateways include all hardware and software used to link dissimilar network operating systems (NOS) or to link local-area networks (LANs) to mainframes or wide-area networks (WANs). Gateways also are used in electronic mail (E-mail) to convert messages between services using different E-mail protocols.

Graphical User Interface (GUI): A GUI uses graphical symbols, called icons, and menu to carry out commands.

Local-Area Network (LAN): A group of computers, usually in one building or office, physically connected in a manner that lets them communicate and interact with each other. For a network to

operate, it needs a server, which is a computer that holds data used by the different computers on the network. Some of the benefits of a network connection include the ability to share document files and expensive equipment. Networks can be connected using different combinations of topologies, protocols, software and hardware. A network that uses radio transmissions instead of cables to connect computers may be called a local-area wireless network.

Media Access Control (MAC): The protocol that determines the transmission of information on a network.

Node: Any device that can communicate with other computers in a group of interconnected computers. Usually, a node refers specifically to a computer system (CS) or terminal that is part of a network.

Packet: A block of data transmitted from one computer to another on a network or on the Internet. A packet contains three parts: the data to be transmitted, the data needed to guide the packet to its destination, and the data that corrects errors that occur along the way. Several packets make up a typical transmission. The computer splits up the transmission at the transmission point and reassembles it at the destination point.

Protocol: A set of rules and procedures for exchanging data between computers on a network or through the Internet. Protocol usually includes information or error checking, data compression, and sending and receiving messages.

Router: The part of a communications network that receives transmissions and forwards them to their destinations using the shortest route available. Data may travel through multiple routers on the way to its destination.

Simple Network Management Protocol (SNMP): It exchanges network information through messages technically known as protocol date units (PDUs).

Telnet: Terminal emulation in which a user is connected to a remote host using an Internet account as if the user were directly connected to the host, such that a connectivity session continues as if the user was at a terminal connected to the host, though the user is actually connected to another site, using the Internet to connect to the host.

Topology: The physical configuration of a network that determines how the network's computers are connected.

Transmission Control Protocol/Internet Protocol (TCP/IP): A language governing communication among all computers on the Internet. TCP/IP is two separate protocols, TCP and IP, that are used together. The Internet Protocol portion of the standard dictates how packets of information are sent out over networks. IP has a packet-addressing method that lets any computer on the Internet forward a packet to another computer that is a step or more closer to the packet's recipient. The Transmission Control Protocol ensures the reliability of data transmissions across Internet-connected networks. TCP checks packets for errors and submits requests for retransmission if errors are found; it also will return the multiple packets of a message into the proper, original sequence when the message reaches its destination.

Wide-Area Network (WAN): A collection of computers connected or networked to each other over a geographic area. WANs usually require special arrangements with telephone companies because data is transmitted among locations (called sites) across telephone lines.

A computer network is simply a collection of autonomous computers connected together to permit sharing of hardware and software resources, and to increase overall reliability. The qualifying term "local area" is usually applied to computer networks in which the computers are located in a single building or in nearby buildings, such as on a college campus or at a single corporate site. When the computers are further apart, the term "wide area network" is used, but the distinction is one of degree and the definitions sometimes overlap.

A bridge is a device that is connected to at least two LANs and serves to pass message frames or packets between LANs, such that a source station on one LAN can transmit data to a destination station on another LAN, without concern for the location of the destination. Bridges are useful network components, principally because the total number of stations on a single LAN is limited. Bridges can be implemented to operate at a selected layer of protocol of the network.

At the heart of any computer network is a communication protocol. A protocol is a set of conventions or rules that govern the transfer of data between computer devices. The simplest protocols define only a hardware configuration, while more complex protocols define timing, data formats, error detection and correction techniques and software structures.

Computer networks almost universally employ multiple layers of protocols. A low-level physical layer protocol assures the transmission and reception of a data stream between two devices. Data packets are constructed in a data link layer. Over the physical layer, a network and transport layer protocol governs transmission of data through the network, thereby ensuring reliable data delivery.

A model for network architectures has been proposed and widely accepted. It is known as the International Standards Organization (ISO) Open Systems Interconnection (OSI) reference model. The OSI reference model is not itself a network architecture. Rather it specifies a hierarchy of protocol layers and defines the function of each layer in the network. Each layer in one computer of the network carries on a conversation with the corresponding layer in another computer with which communication is taking place, in accordance with a protocol defining the rules of this communication. In reality, information is transferred down from layer to layer in one computer, then through the channel medium and back up the successive layers of the other computer. However, for purposes of design of the various layers and understanding their functions, it is easier to consider each of the layers as communicating with its counterpart at the same level, in a "horizontal" direction.

The lowest layer defined by the OSI model is called the physical layer, and is concerned with transmitting raw data bits over the communication channel. Design of the physical layer involves issues of electrical, mechanical or optical engineering, depending on the medium used for the communication channel. The layer next to the physical layer is called the data link layer. The main task of the data link layer is to transform the physical layer, which interfaces directly with the channel medium, into a communication link that appears error-free to the next layer above, known as the network layer. The data link layer performs such functions as structuring data into packets and attaching control information to the packets.

Although the data link layer is primarily independent of the nature of the physical transmission medium, certain aspects of the data link layer function are more dependent on the transmission

medium. For this reason, the data link layer in some network architectures is divided into two sublayers: a logical link control sublayer, which performs all medium-independent functions of the data link layer, and a MAC sublayer. This sublayer determines which station should get access to the communication channel when there are conflicting requests for access. The functions of the MAC layer are more likely to be dependent on the nature of the transmission medium.

The basic function of a bridge is to listen "promiscuously," i.e., to all message traffic on all LANs to which it is connected, and to forward each message it hears onto LANs other than the one from which the message was heard. Bridges also maintain a database of station locations, derived from the content of the messages being forwarded. Bridges are connected to LANs by paths known as "links." After a bridge has been in operation for some time, it can associate practically every station with a particular link connecting the bridge to a LAN, and can then forward messages in a more efficient manner, transmitting only over the appropriate link. The bridge can also recognize a message that does not need to be forwarded, because the source and destination stations are both reached through the same link. Except for its function of "learning" station locations, or at least station directions, the bridge operates basically as a message repeater.

As network topologies become more complex, with large numbers of LANs, and multiple bridges interconnecting them, operational difficulties can ensue if all possible LAN bridging connections are permitted. In particular, if several LANs are connected by bridges to form a closed loop, a message may be circulated back to the LAN from which it was originally transmitted,

and multiple copies of the same message will be generated. In the worst case, messages will be duplicated to such a degree that the networks will be effectively clogged with these messages and unable to operate at all.

Internet is a collection of networks, including Arpanet, NSFnet, regional networks, local networks at a number of university and research institutions, and a number of military networks. The protocols generally referred to as TCP/IP were originally developed for use only through Arpanet and have subsequently become widely used in the industry. The protocols provide a set of services that permit users to communicate with each other across the entire Internet. The specific services that these protocols include file transfer, remote log-in, remote execution, remote printing, computer mail, and access to network file systems.

The basic function of the Transmission Control Protocol (TCP) is to make sure that commands and messages from an application protocol, such as computer mail, are sent to their desired destinations. TCP keeps track of what is sent, and retransmits anything that does not get to its destination correctly. If any message is too long to be sent as one "datagram," TCP will split it into multiple datagrams and makes sure that they all arrive correctly and are reassembled for the application program at the receiving end. Since these functions are needed for many applications, they are collected into a separate protocol (TCP) rather than being part of each application. TCP is implemented in the transport layer of the OSI reference model.

The Internet Protocol (IP) is implemented in the network layer of the OSI reference model, and provides a basic service to TCP: delivering datagrams to their destinations. TCP simply hands IP a

datagram with an intended destination; IP is unaware of any relationship between successive datagrams, and merely handles routing of each datagram to its destination. If the destination is a station connected to a different LAN, the IP makes use of routers to forward the message. TCP/IP frequently uses a slight deviation from the seven-layer OSI model in that it may have five layers. The five layers are as follows:

Layer 5--The Application Layer. Applications such as ftp, ***telnet,*** SMTP, and NFS relate to this layer.

Layer 4--The Transport Layer. In this layer, TCP and UDP add transport data to the packet and pass it to layer 3.

Layer 3--The Internet Layer. When an action is initiated on a local host (or initiating host) that is to be performed or responded to on a remote host (or receiving host), this layer takes the package from layer 4 and adds IP information before passing it to layer 2.

Layer 2--The Network Interface Layer. This is the network device as the host, or local computer, sees it and it is through this medium that the data is passed to layer 1.

Layer 1--The Physical Layer. This is literally the Ethernet or Serial Line Interface Protocol (SLIP) itself.

At the receiving host the layers are stripped one at a time, and their information is passed to the next highest level until it again reaches the application level. If a gateway exists between the initiating and receiving hosts, the gateway takes the packet from the physical layer, passes it through a data link to the IP physical layer to continue. As a message is sent from the first host to the second, gateways pass the packet along by stripping off lower layers, readdressing the lower layer, and then passing the packet toward its final destination.

A router, like a bridge, is a device connected to two or more networks. Unlike a bridge, however, a router operates at the network layer level, instead of the data link layer level. Addressing at the network layer level makes use of a 32-bit address field for each host, and the address field includes a unique network identifier and a host identifier within the network. Routers make use of the destination network identifier in a message to determine an optimum path from the source network to the destination network. Various routing algorithms may be used by routers to determine the optimum paths. Typically, routers exchange information about the identities of the networks to which they are connected.

When a message reaches its destination network, a data link layer address is needed to complete forwarding to the destination host. Data link layer addresses are 48 bits long and no two hosts, wherever located, have the same data link layer address. There is a protocol called ARP (address resolution protocol), which obtains a data link layer address from the corresponding network layer address (the address that IP uses). Typically, each router maintains a database table from which it can look up the data link layer address, but if a destination host is not in this ARP database, the router can transmit an ARP request. Only the addressed destination host responds, and the router is then able to insert the correct data link layer address into the message being forwarded, and to transmit the message to its final destination.

IP routing specifies that IP datagrams travel through internetworks one step at a time based on the destination address in the IP header. The entire route is not known at the outset of the journey. Instead, at each stop, the next destination is calculated by

matching the destination address within the datagram's IP header with an entry in the current node's routing table.

Each node's involvement in the routing process consists only of forwarding packets based on internal information resident in the router, regardless of whether the packets get to their final destination. To extend this explanation a step further, IP routing does not alter the original datagram. In particular, the datagram source and destination addresses remain unaltered. The IP header always specifies the IP address of the original source and the IP address of the ultimate destination.

When IP executes the routing algorithm it computes a new address, the IP address of the device to which the datagram should be sent next. This algorithm uses the information from the routing table entries, as well as any cached information local to the router. This new address is most likely the address of another router/gateway. If the datagram can be delivered directly, the new address will be the same as the destination address in the IP header.

The next address defined by the method above is not stored in the IP datagram. There is no reserved space to hold it and it is not "stored" at all. After executing the routing algorithm to define the next step address to the final destination. The IP protocol software passes the datagram and the next step address to the network interface software responsible for the physical network over which the datagram must now be sent.

The network interface software binds the next step address to a physical address, forms a packet using the physical address, places the datagram in the data portion of the packet, and sends the result out over the physical network interface through which the next step gateway is reached. The next gateway receives the datagram and

the foregoing process is repeated. In addition, the IP does not provide for error reporting back to the source when routing anomalies occur. This task is left to another Internet protocol, the Internet Control Message Protocol (ICMP).

A router will perform protocol translation. One example is at layers 1 and 2. If the datagram arrives via an Ethernet interface and is destined to exit on a serial line, for example, the router will strip off the Ethernet header and trailer, and substitute the appropriate header and trailer for the specific network media, such as SMDS, by way of example.

A route policy may be used instead of routing table entries to derive the next step address. In the system and methodology of the present invention, the source address is tested to see in which ISP address range it falls. Once the ISP address range is determined the packet is then routed to the next step address associated with the specific ISP.

It must be noted, however, that routing wired networks at connection nodes is the most efficient means of passing Internet data. One aspect of the present wireless provisioning router is to provide routing at each node connection point. This provides for a stronger network and provides flexibility in network design. This flexibility allows for better network traffic management and improves the overall bandwidth by reducing network latency through optimization of routes and data packet management. Although the wireless provisioning router is capable of bridging, it will be the determination of the network engineer to establish the wireless provisioning router as a bridge to the network or a router to the network. This feature gives the network engineer more flexibility to determine the network design. Furthermore, the flexible nature of the

equipment allows the user to change a leaf node that bridges into a major backbone node that routes through the use of code modification without the need to reboot.

Subsequently, as a node begins to grow, the network engineer can upgrade that node to fit the needs of the network without harming existing customers. By inserting the cards in the slots of a chassis that contains open-source preferably LINUX, as its operating system (OS), the wireless provisioning router can be configured as a router or a bridge. The routing model of LINUX is not a portion of the main operating kernel. Being a subcomponent of the OS, the routing module can be upgraded and modified without rebooting the system. A reboot of an advanced LINUX box may take up to 30 minutes to complete. The upgrade of a routing module in LINUX takes less than 2 seconds to reinitialize. This reinitialization is transparent to the customers attached to this box. The routing module is replaceable by a bridge module if routing is not necessary for the connection node. Routing at the connection point allows for the filtering of IP addresses for either all of the customers attached to that node or for an individual IP address attached to that node. Furthermore, the routing module contains routing logic capable of bandwidth shaping. This process only allows certain volumes of data to be transmitted to and/or from a certain customer IP address.

Ultimately in network information systems it has been shown that users do not know what they do not know. The only static feature is that the user knows what should be happening. By applying rule sets to the SARPed provisioning device the user can specify what the network datagrams should look like. All other data is assumed hostile in nature. Known nefarious behavior results in port and IP address blocking from the source of the attacker. Behavior outside the range

of predicted activity is scored and returned to the network security officer for review. This method removes the responsibility of detecting virus, spyware and other unwanted datagrams from the local host and places the responsibility on the edge point router. The local host is typically managed by customers that are not highly trained in network maintenance. The edge point router is managed by highly trained network engineers.

When traffic comes to the provisioning device each datagram is reviewed by signature. Some signatures such as SNMP and ICMP sweeps are not so bad and we do not take action against those activities however we log those and report the source IP so a user can monitor the traffic. Other datagrams are clearly bad. For instance the Code Red virus sends a data request to port 80 of a web server and it looks something like default.ida?xxxxxxxxxxxxxxxxxxxxxxxx..... These types of datagrams result in a socket reset and 5 minute block of the user to the provisioning device. In the event the datagram does cause a buffer overflow which is the purpose of this attack, the socket is broken and the attacker does not have access to the hack. Once the socket is broken the hack is over. Furthermore spyware like keyloggers and trojans can be hard to detect on your system. However the outbound data is clear. Typically these methods involve non-standard ports. For instance port 17300 or port 23000 are both examples of trojan horse ports. Keyloggers are a little different. These can use typical ports like 80 and 22 and 23. However, they connect to distant ip addresses that have no DNS resolution. Furthermore these methods also maintain a sense of schedule and are not as random as user traffic. Finally these methods will attempt to transmit even when a user is logged off. By leaving the computer powered on yet not logged into the network, it

is possible to detect nefarious behavior because of the nature of the IP tables and dynamic routing process the computer believes there is connectivity to the outside world.

An apparatus and system according to the invention works well in a wide variety of cases and does not inhibit or impact future enhancements to network protocols and operating systems. To assure that operations at the application and transport levels do become aware of changes of address promptly, the apparatus and system may eliminate the prospect of a single point of failure, eliminate or reduce sub-optimal routing for all applications, provide improved security to protect communication over wireless media, and allow users to switch network adapter cards while preserving all connections, such as software applications and network administration, transparently to the user.

With respect to the filtering function of the provisioning device, all data must travel to from the user's PC to the route controller through an IPSEC tunnel created before authentication takes place, which makes auditing and IDS more robust due to the fact that all data packets are evaluated by an intelligent router.

A bad packet list is created and the route controller only lets packets through that are not on the list. The IDS system detects source, destination of the packet. Individually benign data may be allowed through but as a coordinated group of data's score increases to a predefined score parameter during a predefined period of time, subsequent access is blocked. This differs from conventional systems in that the audit function is not localized allowing the every data packet to be screened at the same location. Alternatively, the packets can be accessed first by the route controller.

IEEE ***802.11*** is a standard for wireless systems that operate in the 2.4-2.5 GHz ISM (industrial, scientific and medical) band. This ISM band is available worldwide and allows unlicensed operation for spread spectrum systems. For both the US and Europe, the 2,400-2,483.5 MHz band has been allocated, while for some other countries, such as Japan, another part of the 2.4-2.5 GHz ISM band has been assigned. The ***802.11*** standard focuses on the MAC (medium access control) protocol and PHY (physical layer) protocol for access point (AP) based networks and ad-hoc networks. WiFi generally refers to the ***802.11b*** standard.

In access point based networks, the stations within a group or cell can communicate only directly to the access point. This access point forwards messages to the destination station within the same cell or through a wired distribution system to another access point, from which such messages arrive finally at the destination station. In ad-hoc networks, the stations operate on a peer-to-peer level and there is no access point or (wired) distribution system.

The ***802.11*** standard supports: DSSS (direct sequence spread spectrum) with differential encoded BPSK and QPSK; FHSS (frequency hopping spread spectrum) with GFSK (Gaussian FSK); and infrared with PPM (pulse position modulation). These three physical layer protocols (DSSS, FHSS and infrared) all provide bit rates of 2 and 1 Mbit/s. The ***802.11*** standard further includes extensions 11a and 11b. Extension 11b is for a high rate CCK (Complementary Code Keying) physical layer protocol, providing bit rates 11 and 5.5 Mbit/s as well as the basic DSSS bit rates of 2 and 1 Mbit/s within the same 2.4-2.5 GHz ISM band. Extension 11a is for a high bit rate OFDM (Orthogonal Frequency Division Multiplexing) physical layer protocol standard providing bit rates in the range of 6 to 54 Mbit/s in the 5 GHz band.

The ***802.11*** basic medium access behavior allows interoperability between compatible physical layer protocols through the use of the CSMA/CA (carrier sense multiple access with a collision avoidance) protocol and a random back-off time following a busy medium condition. In addition all directed traffic uses immediate positive acknowledgement (ACK frame), where a retransmission is scheduled by the sender if no positive acknowledgement is received. The ***802.11*** CSMA/CA protocol is designed to reduce the collision probability between multiple stations accessing the medium at the point in time where collisions are most likely occur. The highest probability of a collision occurs just after the medium becomes free, following a busy medium. This is because multiple stations would have been waiting for the medium to become available again. Therefore, a random back-off arrangement is used to resolve medium contention conflicts. In addition, the ***802.11*** MAC defines: special functional behavior for fragmentation of packets; medium reservation via RTS/CTS (request-to-send/clear-to-send) polling interaction; and point co-ordination (for time-bounded services).

The IEEE ***802.11*** MAC also defines Beacon frames, sent at a regular interval by an AP to allow wireless stations (STAs) to monitor the presence of the AP. IEEE ***802.11*** also defines a set of management frames including Probe Request frames which are sent by an STA, and are followed by Probe Response frames sent by the AP. Probe Request frames allow an STA to actively scan whether there is an AP operating on a certain channel frequency, and for the AP to show to the STA what parameter settings this AP is using.

IEEE 802.11 is a shared, wireless local area network (LAN) standard. It uses the carrier sense multiple access (CSMA), medium access control (MAC) protocol with collision avoidance (CA). This

standard allows for both direct sequence (DS), and frequency-hopping (FH) spread spectrum transmissions at the physical layer. The maximum data rate initially offered by this standard was 2 megabits per second. A higher-speed version, with a physical layer definition under the IEEE 802.11b specification, allows a data rate of up to 11 megabits per second using DS spread spectrum transmission. The IEEE standards committee has also defined physical layer criteria under the IEEE 802.11a specification. This is based on orthogonal frequency-division multiplexing (OFDM) that will permit data transfer rates up to 54 megabits per second.

While IEEE 802.11 has experienced a rapid growth in the wireless local area network LAN environment, a number of security concerns have been raised for wireless networks in general. The IEEE 802.11 wireless LAN standard defines authentication and encryption services based on the Wired Equivalent Privacy (WEP) algorithm. The WEP algorithm defines the use of a 40-bit secret key for authentication and encryption. Many IEEE 802.11 implementations also allow 104-bit secret keys. However, the standard does not define a key management protocol, and presumes that the secret, shared keys are delivered to the IEEE 802.11 wireless station via a secure channel independent of IEEE 802.11.

The lack of a WEP key management protocol is a principal limitation to providing IEEE 802.11 security; especially in a wireless infrastructure network mode with a large number of stations. The lack of authentication and encryption services also effects operation in a wireless, ad hoc network mode where users may wish to engage in peer-to-peer collaborative communication; for example, in areas such as conference rooms.

As a result, the enhanced importance of authentication and encryption, in a wireless environment, proves the need for access control and security mechanisms that include the key management protocol specified in IEEE 802.11.

It has been shown that routing wired networks at connection nodes has long stood as the most efficient and secure means of passing Internet data. However, this method uses upgrades to old voice networks. The wired solution will never be useful for providing service to the mobile user. However, to date wireless Internet Access has been sought but security, limitation of service and mobile IP stand in the way of this solution for mobile broadband.

The WPDWAN has evolved the following features that address these concerns. The first aspect of the WPDWAN is contained in the mobile Authentication method. Using the Lightweight Directory Access Protocol (LDAP) authentication schema, a user of the present system and method is able to control the network in a manner not traditionally considered for a data network.

The LDAP device contains user profiles. That directory is broken into sections by user type such as customer and employee. These types have sub groups such as location where service is initiated and where the individual is allowed to obtain access on the network. This tree also allows for the control of bandwidth and can even be defined to the time of day that the allotted bandwidth can be distributed.

The LDAP server works in conjunction with a DHCP server that has been modified for the purpose of this network. Connection to the radio network is a complex matter that does not in itself provide network connectivity. The LDAP server tests the connection to the radio network for the Manufacture Access Code (MAC) address. This

number is transmitted in each data pack and is compared to the value stored in the user profile. If the two match the DHCP server authorizes an IP address for delivery to the user connecting.

This method of authentication at this point is rather simple to penetrate. By guessing the address block served by the DHCP server the user can guess an address on the block and enter into the network. However, the present inventor made one other modification to the network in that all traffic on the local node for the wireless must pass through a route controller computer. This box has a limited number of active routes. These routes are established and removed by the DHCP software. When a lease is activated the route is created. If the lease expires the route is removed. Certain tests are run throughout the process to determine if the customer has discontinued use of the lease before the expiration of the lease. In this case the route is also removed after the lease is determined vacant for 5 minutes. The vacancy time takes into consideration the transit between cells to insure the client ample time to travel between connection points without disruption of the socket layer.

The LDAP feature provides two significant differences to the RADIUS method implement through CHAP or PPPOE. The first significant change prevents the authentication method from violating an effect of the 802.IIb protocol. The LDAP route controller method allows the user to transit from tower to tower without interruption at the socket layer. This means seamless transitions between towers will result. The socket layer connection maintenance insures the user can maintain connections for streaming video and audio as well as SMTP traffic.

Scalability is also a feature an exemplary embodiment of the present invention. The LDAP standard provides for a distributed replication method of data. As the user set grows more and more

requests will be made for authentication. Because the LDAP solution natively supports distributed replication, the user information can be loaded into a machine local to his border point to the Internet cloud. This information will propagate to the master LDAP server and then be propagated throughout the network. However, when requests for authentication occur on a fully operational network the request for authentication will only be made at the border point. This reduces overall network traffic to the Internet cloud and increases throughput to the user. This also reduces computer capacity in local areas by distributing the load to the replica machines at each Macro cell. This reduces cost of the system. In the case that one component of the network fails, the replication feature allows other components to pick up the failure and solve the problem until a repair can be made. This eliminates single point failures of authentication.

The next essential component of an exemplary WPDWAN is the customer premise equipment, namely the wireless provisioning device. It is a router with a wireless interface. A preferred embodiment of the wireless provisioning device is provided in co-pending U.S. Patent Application Serial No.09/660,709, which is incorporated herein by this reference. The wireless provisioning device can control bandwidth speed and data type as well as provide firewall capability.

One aspect of the wireless provisioning router is to provide routing at each node connection point. This aspect provides for a stronger network and provides flexibility in network design. This feature allows for better network traffic management improving the overall bandwidth by reducing network latency through the optimization of routes and data packet management. Although the wireless provisioning device is capable of bridging it will be the determination

of the network engineer to establish the wireless provisioning device as a bridge to the network or a router to the network. This feature gives the network engineer more flexibility to the network design. Furthermore the flexible nature of the equipment allows the user to change a leaf node that bridges into a major backbone node that routes through the use of code modification without the need to reboot. Subsequently as a node begins to grow the network engineer can upgrade that node to fit the needs of the network without banning existing customers. By inserting the cards in the slots of a chassis that contains open source LINUX as its operating system (OS), the wireless provisioning device can be configured as a router or a bridge. The routing model of LINUX is not a portion of the main operating kernel. Being a sub component of the OS, the routing module can be upgraded and modified without rebooting the system. A reboot of an advanced LINUX box may take up to 30 minutes to complete. The upgrade of a routing module in LINUX takes less than 2 seconds to reinitialize. This re-initialization is transparent to the customers attached to this box. The routing module is replaceable by abridging module if routing is not a necessity for the connection node. Routing at the connection point allows for filtering of IP addresses for either all the customers attached to that node or for an individual IP address attached to that node. Furthermore the routing module contains routing logic capable of bandwidth shaping. This process only allows certain volumes of data to be transmitted to and/or from a certain customer IP address. Because of the LDAP structure this bandwidth allotment is controlled through the profile of the user as established on the LDAP server.

The second feature of the WPDWAN revolves around the addition of more access points. Through the use of wireless

provisioning device integration to the system a flexible configuration is introduced. The wireless provisioning device may contain up to 7 wireless connections and 1 wired connection, or 7 wired connections and 1 wireless connection or any combination as seen fit for the network or alternative be configured with a microprocessor chipset that allows for an indeterminate number of connections while allowing for the miniaturization of the provisioning device. This reduces overall cost and decreases space requirements. By placing this system on a faster chip set the equipment effectively processes more data from the same point. Furthermore this feature allows the expansion of the system to develop from an outlying leaf node with little usage to a major backbone node with multiple redundancy without affecting existing customers. The user can also increase the number of potential customers to the connection point in the network by adding cards and antennas without the need for chassis changes. Because the physical configuration of the system resides in a chassis of a microcomputer, the wireless provisioning device can be configured with differing numbers of wireless cards and network cards. The chassis may contain a multiplicity of processors. In preferred embodiments, the device and/or system runs on a UNIX based system but may employ alternative operating systems that may be satisfactory for hefty data management. This processor configuration and extensive amounts of RAM memory allows the operating system to handle extensively more information than the traditional wireless connection points.

The increased functionality of the wireless provisioning device also modifies the IP assignment of the WPDWAN. As a third feature of the WPDW AN, DHCP is used to assign all mobile users, and most static users of the service. Static IP's may also be added for large static

customers when IP allocation is a requirement. Because DHCP is a second layer protocol, routed networks cannot pass DHCP assignment through a router. However, the WPDWAN design incorporates the wireless provisioning device design as either a bridge or router. When acting as a bridge or switch the DHCP allocation passes through the wireless provisioning device to the customer machine seamlessly. However, when the wireless provisioning device is acting as a router the DHCP assignment must come from the wireless provisioning device itself. To logically segment the network in such a fashion as to provide each wireless provisioning device with an IP block is cumbersome. Since the routers can all slave to master BGP routers, advanced tables may be created on the BGP routers or other servers to provide dynamic segmentation to the wireless provisioning device. Therefore, segments can be created that optimized IP addressing as users enter and exit the network.

The WPDWAN centers on the security of the wireless network. Each wireless provisioning device is capable of running an ISO-4 standard encryption package capable of creating a VPN to a VPN host located at the border router. This solution prevents traffic from being intercepted while in the wireless network.

Further securing the wireless provisioning device is the method of hiding the wireless provisioning device through the route controller. All connections on the client side of the wireless provisioning device are provided routes to the wireless provisioning device, however routes to both interfaces of the wireless provisioning device are removed from the route controller. The wireless provisioning device can only be accessed when one or both of these routes are added to the route controller box. Using a secure shell telnet connection to the wireless provisioning device, message traffic and administrative

information cannot be sniffed by public domain users on the network. Due to this feature WPDWAN can be made available. This feature uses a more universal management schema of telnet. The WPDWAN is administrated using secure shell telnet integrated with an HTML browser script written in, for example, PERL. Connection to all management nodes is limited to authorized IP addresses, reducing the chances of unauthorized network entries. Present day wireless equipment utilizes the SNMP V -1 protocol for the management of the connection device. SNMP V-I is limited to clear text message traffic. Any connection made to this connection point is on the same logical segment as those that are doing administrative work to the connection device. In every network solution logical segments contain all the information that is passed within that segment. Sniffing traffic on that logical segment has long been known to be a problem within networking. SNMP V –6 protocol is the typical solution to this problem while using SNMP protocol. However, SNMP V -6 is a processor intense protocol providing for extensive network overhead. By using a secure telnet connection the network overhead is reduced while increasing the security of the system. A secure telnet connection only allows certain IP's to connect to certain data ports. This limited connection structure effectively creates different logical segments within the same physical network segment. The newly created logical segment prevents the sniffing of administrative traffic by the common user. Furthermore the shell connection is managed by an HTML based GUI. To date virtually all WPDWAN have the connection points managed by proprietary Windows™ based GUIs. These GUIs allow for the management of one Node at a time. The WPDWAN GUI can manage several nodes at any given time. The user can sort through several diagnostic processes to insure problems are

limited to certain areas and not pervasive throughout the network. This method of management is more intuitive and more complete previously developed WPDWAN.

The WPDWAN is capable of removing limited static MAC addressing and the inclusion of RADIUS authentication. The RADIUS authentication is tied to the MAC addressing in conjunction with a username and password. This method of authentication greatly reduces the chances of service theft and allows the user a mobile solution between cells assuming the resolution of mobile IP. Furthermore this feature lends itself to a directory services method that allows a more customized interface for the user. Using IP filtering, authorization levels and enterprise user management the WPDWAN with directory service has the ability to control bandwidth consumption, and provide a more custom service to the user. Without RADIUS authentication users connect to the network without any control from a central server. By providing RADIUS one server controls the abilities of the user to enter certain parts of the network.

The WPDWAN allows connections from both single PC cards and from other wireless provisioning devices. Through the use of this feature the same WPDWAN may contain single users and large LANs. In present day wireless WANs, the user must choose to provide service to either PC's containing the cards or to a wireless connection bridge. Commercial users would then select to use a wireless connection bridge while a residential user may choose to use a PC. Without the wireless provisioning device, multiple WPDWANs have to be erected to satisfy all types of customers. The WPDWANs incorporation of the wireless provisioning device allows the user to connect to the wireless infrastructure using either an individual PC on the Internet Cloud or another WPDWAN connection point as authorized by the connection

point device. In this case one WPDWAN may be erected while satisfying all potential customer types.

The WPDWAN has the ability to deal with mobile IP. By removing the BGP routing component one layer from all the wireless routers, users are able to float between multiple out -point connections. Since the BGP is broadcast to all other BGP routers in the WPDW AN, all users may move from point to point while the routers broadcast handoffs and modify traffic flow. In other WPDWAN the user will be limited to one outflow period, unless the user reboots the machine. The BGP handoff is valid for DHCP served IP addresses or static IPs provided the IP address has been entered into the BGP table.

The WPDWAN also utilizes 2.4Ghz unlicensed spread spectrum wireless equipment. Large scale routed WANs to date have been developed using either wired technology or some licensed frequency. In both cases the infrastructure costs have been extremely high for both the network owner and the end user. The wired WANs have not been able to provide any mobile ability. The licensed frequencies are extremely expensive and very limited in design. Furthermore efforts in these spectrums have not advanced the bandwidth transmissions to the rates we have developed.

Specific reference is made to US patent application serial numbers 09/660,709, 10/223,255, 60/496,088 and 60/539,242 filed September 13, 2000, August 15, 2002 and August 18, 2002 and January 26, 2004 respectively, which are incorporated, in their entirety, herein by this reference.

Referring specifically to FIG. 1, a system is shown that allows for the monitoring of devices remotely as well as the authentication of network traffic through a wireless provisioning device. In preferred

embodiments, a device that could be any electronic apparatus from a PDA to an implantable medical device is provided that has a unique identifier. The unique identifier could be an IMEI, IMSI or other coding convention that allows each device and/or user to be separately identified. Through the wireless security protocol of the present invention, a device may be located, via a global positioning mechanism tied to the unique identifier, or controlled functionally from a remote location. In such instances it is preferable that a system is provided comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to control remotely a device through secure, authenticated, mobile wireless public domain wide area communications network, using the 802.11 spectrum, said steps comprising: extracting from the device a start session message containing user identity and/or location information, the start session message being received by a controller using the communications network in accordance with a control protocol, the start session message being sent automatically; and sending to the device a control message to control the functionality of the device remotely, the control message being sent from the controller using the communications network in accordance with the control protocol and in response to the start session message, wherein the control message is a session authorization message that determines the functionality of the device.

In the figure, remote device 320 communications via a communication network 300 through the management module 310. As stated above, the remote device may be a wide variety of devices. In certain embodiments, the device may be a home computer 380, a LAN 370 or series of devices 320 connected via a

WAN facilitated by a service provider 340 or a business 350 with its own provisioning system 360, all of which may be connected through a series of towers 330.

The user may monitor the remote device from a management station physically remote from the remote device, such that the management station communicates with the remote device via a communications network and/or a global positioning system. In the event that the communication system is down, the device may continue to be monitored via the global positioning system.

The present invention may be embodied in other specific forms without departing from its spirit or essential characteristics. The described embodiments are to be considered in all respects only as illustrative, and not restrictive. The scope of the invention is, therefore, indicated by the appended claims, rather than by the foregoing description. All changes, which come within the meaning and range of equivalency of the claims, are to be embraced within their scope.

CLAIMS

What is claimed is:

1. A method of providing secure, authenticated, mobile client access to a wireless public domain wide area network, using the 802.11 spectrum, without resort to a client side driver, comprising the steps of:

receiving from a client a start session message containing user identity information, the start session message being received by the route controller using the communications network in accordance with a client control protocol, the start session message being sent automatically upon the client being logged on to the service provider independent of the client controller; and

sending to the client a control message to control the client's access to use the communications network, the control message being sent from the route controller using the communications network in accordance with the client control protocol and in response to the start session message.

2. The method of claim 1, further comprising the step of: routing or bridging the user identity information through a wireless provisioning routing device.

3. The method of claim 1, wherein said step of sending controls whether the client is authorized or denied access to use the communications network.

4. The method of claim 3, wherein the control message is a session authorization message authorizing the client to use the communications network for a predetermined period of time.

5. The method of claim 3, wherein the control message is a session authorization message authorizing the client to use the communications network at a predetermined bandwidth level.

6. The method of claim 5, further comprising the step of:

determining if the client is authorized to use the communications network based on the user identity information, and wherein said step of sending a session authorization message is only performed if the client is authorized to use the communications network.

7. The method of claim 5, further comprising the steps of:

receiving from the client a session continuation message containing the user identity information; and

sending to the client a continuation authorization message, based on the user identity information, authorizing the client to use the communications network for an additional predetermined period of time.

8. The method of claim 7, wherein the continuation authorization message is an additional session authorization message.

9. The method of claim 7, further comprising the step of determining if the client is authorized to continue to use the communications network based on the user identity information, and wherein said step of sending a continuation authorization message is only performed if the client is authorized to continue using the communications network.

10. The method of claim 3, further comprising the step of:

determining if the client is authorized to use the communications network based on the user identity information; and

wherein the control message is a deny session message if the client is not authorized to use the communications network.

11. The method of claim 1, further comprising the step of sending to the client an additional control message that instructs the client to display a message to a user.

12. The method of claim 1, further comprising the step of sending to the client an additional control message that instructs the client to receive data.

13. The method of claim 1, further comprising the steps of:

recording information about a client session in a communications network usage log.

14. The method of claim 13, wherein the recorded information includes information associated with the user identity information and information associated with the time that the client session started.

15. The method of claim 13, further comprising the steps of:

receiving from the client an end session message containing the user identity information; and

recording information about the end of the client session in the usage log.

16. The method of claim 13, further comprising the step of: recording information about an end of the client session in the usage

log if no session continuation message has been received from the client during the predetermined period of time.

17. The method of claim 13, further comprising the steps of: receiving from the service provider a communications network usage report; and comparing the communications network usage report with the communications network usage log to determine discrepancies.

18. The method of claim 1, further comprising the steps of: sending to the client a session termination message instructing the client to end the client session; and recording information about the end of the client session in a usage log.

19. A method using a route controller to monitor a remote device, comprising the steps of:

accessing a remote device based on an international identifier;

receiving from a remote device a start session message containing user identity and/or location information, the start session message being received by the controller using the communication network in accordance with a client control protocol, the start session message being sent automatically upon accessing the remote device;

recording in a communications network usage log information associated with the user identity information and information associated with the time that the start session message was received and the location of the device; and

sending to the client, in response to the start session message, a control message to control the functionality of the device.

20. The method of claim 19, wherein the remote device is selected from the group consisting of computers, automobiles, aircraft, medical devices, or combinations thereof.

21. An apparatus for providing secure, authenticated, mobile wireless client access to use a wireless public domain wide area communications network, utilizing the 802.11 spectrum, comprising:

means for receiving from the client a start session message containing user identity information, the start session message being received by the client controller using the communications network in accordance with a client control protocol, the start session message being sent automatically upon the client being logged on to the service provider independent of the client controller;

means for determining if the client is authorized to access the communications network; and

means for sending to the client a session authorization message, the session authorization message to control the client's access to use the communications network being sent from the client controller using the communications network in accordance with the client control protocol and in response to the start session message.

22. The apparatus of claim 21, wherein the session authorization message controls whether the client is authorized or denied access to use the communications network.

23. The apparatus of claim 21, wherein the session authorization message authorizes the client to use the communications network for a predetermined period of time.

24. The apparatus of claim 21, wherein the communications network is the Internet and the client control protocol is an in-band protocol transmitted using transmission control protocol/Internet protocol.

25. An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to control remotely a device through secure, authenticated, mobile wireless public domain wide area communications network, using the 802.11 spectrum, said steps comprising:

extracting from the device a start session message containing user identity and/or location information, the start session message being received by a controller using the communications network in accordance with a control protocol, the start session message being sent; and

sending to the device a control message to control the functionality of the device remotely, the control message being sent from the controller using the communications network in accordance with the control protocol and in response to the start session message, wherein the control message is a session authorization message that determines the functionality of the device.

26. A method of providing ARP tactic resistant network security for, comprising the steps of:

providing a network utilizing an Address Resolution Protocol and public/private key encryption, the network having

at least one client computer and at least one provisioning device;

passing the public and private keys between the at least one client computer and the at least one provisioning device to initiate the session; and

auditing the session through a policy table accessible to both the at least one client computer and the at least one provisioning device;

whereby the Address Resolution protocol can be turned off without having to resort to static routes and static Address Resolution Protocol entry on each client computer.

27. An apparatus for providing ARP tactic resistant network security, comprising:

means for receiving and reviewing each datagram by signature;

means for determining if the datagram is authorized to enter or exit the communications network; and

means for initiating socket reset for packets determined to have achieved unauthorized access.

28. A method of providing secure, authenticated, mobile client access to a WiFi Spectrum network, without resort to a client side driver, comprising the steps of:

receiving from a client a start session message containing user identity information, the start session message being received by the route controller using the communications network in accordance with a client control protocol, the start session message being sent automatically upon the client being

logged on to the service provider independent of the client controller; and

sending to the client a control message to control the client's access to use the communications network, the control message being sent from the route controller using the communications network in accordance with the client control protocol and in response to the start session message.

29. A route controller to control a client's access to use a wireless wide area communications network, the route controller comprising:

a communications port capable of receiving from the client a start session message containing user identity information, the start session message being received by the client controller using the communications network in accordance with a client control protocol, the start session message being sent automatically upon the client being logged on to the service provider independent of the client controller;

a user database containing information associated with the user identity information; and

a client control processor coupled to said communications port and said user database, said client control processor being configured to send a control message to the client to control the client's access to use the communications network, the control message being sent from the client controller using the communications network in accordance with the client control protocol and in response to the start session message;

wherein the control message control message is a session authorization message that determine whether the client is granted or denied access to use the communications network for a predetermined period of time.

30. The client controller of claim 29, wherein the route controller is housed on a single chip.

31. An apparatus for providing secure, authenticated, mobile wireless client access to use a WiFi spectrum network, comprising:

means for receiving from the client a start session message containing user identity information, the start session message being received by the client controller using the communications network in accordance with a client control protocol, the start session message being sent automatically upon the client being logged on to the service provider independent of the client controller;

means for determining if the client is authorized to access the communications network; and

means for sending to the client a session authorization message, the session authorization message to control the client's access to use the communications network being sent from the client controller using the communications network in accordance with the client control protocol and in response to the start session message.

32. The apparatus of claim 31, wherein the apparatus is housed within a chassis.

33. The apparatus of claim 31, wherein the apparatus resides on a single chip.

34. An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to control a client's access to use a secure, authenticated, WiFi spectrum network, said steps comprising:

receiving from the client a start session message containing user identity information, the start session message being received by the client controller using the communications network in accordance with a client control protocol, the start session message being sent automatically upon the client being logged on to the service provider independent of the client controller; and

sending to the client a control message to control the client's access to use the communications network, the control message being sent from the client controller using the communications network in accordance with the client control protocol and in response to the start session message, wherein the control message control message is a session authorization message that determine whether the client is granted or denied access to use the communications network for a predetermined period of time.

35. A method of using a communications network having a route controller, comprising the steps of:

accessing the route controller though a service provider independent of the client controller;

sending to the route controller a start session message containing user identity information, the start session message

being sent automatically upon being logged on to the service provide; and

receiving from the route controller a control message to control whether the client is authorized or denied access to use the communications network, the control message being received by the client using the communications network in accordance with a client control protocol and in response to the start session message, wherein the control message control message is a session authorization message that determine whether the client is granted or denied access to use the communications network for a predetermined period of time.

36. An article of manufacture comprising a computer-readable medium having stored thereon instructions adapted to be executed by a processor, the instructions which, when executed, define a series of steps to use a communications network having a route controller, said steps comprising:

accessing the route controller through a wireless communication entry point;

sending to the route controller a start session message containing user identity information,; and

receiving from the route controller a control message to control whether the client is authorized or denied access to use the communications network, the control message being received by the client using the communications network in accordance with a client control protocol and in response to the start session message.

37. A remote device comprising: a unique identifier; a network interface; a manager in communication with the network

interface; wherein the manager interacts via the network interface to a network with that utilizes the unique identifier.

38. A communications system comprising: a communications network and a remote device comprising: a device unit having a communications network interface; and a management module in communication with the device unit and connected to communication network; wherein the management module operates a management communications channel over the communication network and sends location and receives operating instructions from a remote operator via the communications network.

39. A method of managing a remote device, wherein the remote device comprises: a device unit having a communications network interface; a global positioning locator; a management module in communication with the device unit, the management module being passively connectable to a communication network and the global positioning locator; and wherein the management module operates a management communications channel over the communications network and sends location and receives operating instructions; the method comprising the step of:

monitoring the remote device from a management station physically remote from the remote device, wherein the management station communicates with the remote device via a communications network and/or a global positioning system; and in response to a failure of the communications network, continuing monitoring via the global positioning system.

40. The method of claim 39, further comprising the step of communicating monitoring information from the remote device to the management module.

41. The method of claim 40, further comprising the step of querying the remote device to determine operating status.

42. The method of claim 41, further comprising the step of communicating the operating status of the remote device to the management station.

43. The method of claim 39, further comprising the step of providing a signal to the remote device from the management module, wherein the signal provides instructions for the remote device to change state.

44. The method of claim 39, further comprising the step of providing a signal to the remote device from the management module, wherein the signal provides instructions for the remote device to change a control variable.

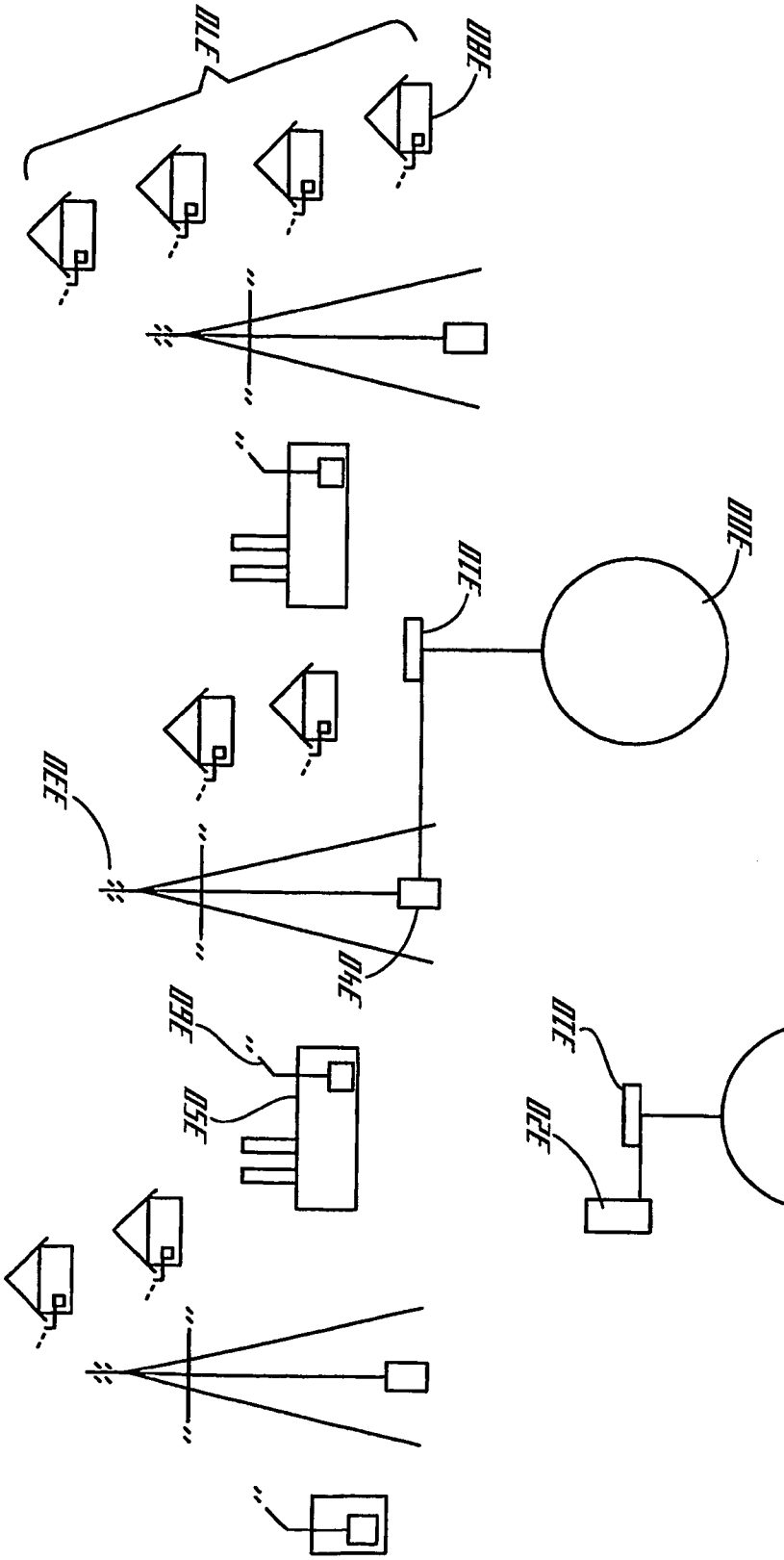


FIG. 1

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 March 2005 (17.03.2005)

PCT

(10) International Publication Number
WO 2005/024567 A3

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number:
PCT/US2004/026809

(22) International Filing Date: 18 August 2004 (18.08.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/496,088	18 August 2003 (18.08.2003)	US
60/539,242	26 January 2004 (26.01.2004)	US
60/581,507	21 June 2004 (21.06.2004)	US

(71) Applicants and
(72) Inventors: **SPEARMAN, Anthony, C.** [US/US]; Route 2, Box 39, Lane, SC 29564 (US). **WASHBURN, E., Russell, III** [US/US]; 3709 Church Street Ext., Roebuct, SC 29376 (US).

(74) Agent: **ALEXANDER, Tony, D.**; Post Office Box 1728, Evans, GA 30809 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

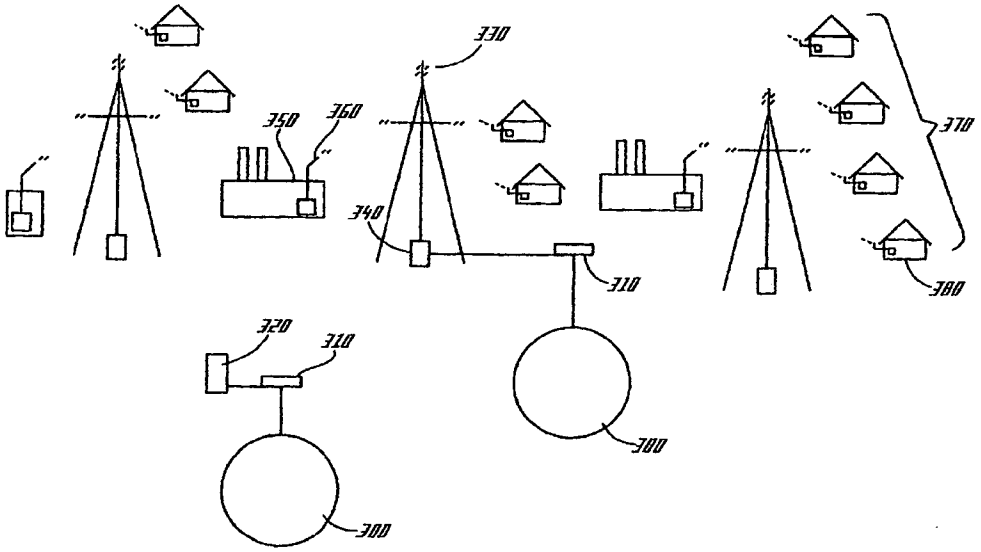
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*
— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for all designations*
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search report*

[Continued on next page]

(54) Title: NETWORK COMMUNICATION SECURITY SYSTEM, MONITORING SYSTEM AND METHODS



(57) Abstract: A system and method of intrusion detection and stoppage that prevents ARP spoofing while preserving the dynamic nature of the network. In particular, a method of turning off ARP without having to resort to static routes and static ARP entry on each computer is provided. Moreover, the system and methods provide for content filtering of both text and images and remote device monitoring and actuation.

WO 2005/024567 A3

(88) Date of publication of the international search report:
4 August 2005

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/26809

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00
US CL : 713/200
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/182

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2003/0120663 A1 (Vining et al) 26 June 2003 (26.06.2003), paragraph 0005.	15-18
X --- Y	US 6,601,171 B1 (CARTER et al) 29 July 2003 (29.07.2003), abstract, column 1, lines 13-21, column 7, line 38 through column 9, line 17, column 9, line 66 through column 12, line 49, and figure 2, 6, and 8.	1-14, 19-25, 28-38 --- 15-18
X	US 2002/0019933 A1 (FRIEDMAN et al) 14 February 2002 (14.02.2002), abstract, paragraph 0079 through paragraph 0189, and figures 4-11.	26 and 27

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
20 April 2005 (20.04.2005)

Date of mailing of the international search report
11 MAY 2005

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703) 305-3230

Authorized officer
for Michelle R. Gao
Ayaz Sheikh

Telephone No. 571-272-2100

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/26809

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
Please See Continuation Sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest
☐ The additional search fees were accompanied by the applicant's protest.
☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US04/26809

BOX III. OBSERVATIONS WHERE UNITY OF INVENTION IS LACKING

This application contains the following inventions or groups of inventions which are not so linked as to form a single general inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claim(s) 1-18, 21-25, 28, and 31-34, drawn to secure access.

Group II, claim(s) 19, 20, 26, 27, 29, 30, 35, and 36, drawn to monitoring a device.

Group III, claim(s) 37-44, drawn to an actual device.

The inventions listed as Groups I, II, and III do not relate to a single general inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: Group I pertains to secure access of a client device, which prevents/permits based on supplied information,
Group II pertains to monitoring a remote device, where information is recorded in a log or database, and
Group III pertains to a physical device, where the device can be claimed by itself, or used within another invention.